

~~SEALED~~
United States District Court

WESTERN DISTRICT OF TEXAS

In the Matter of the Search of

SEARCH WARRANT

Information associated with
kevinpelayo@hotmail.com, further described in
Attachment A, that is stored at premises
controlled by Microsoft Corporation

CASE NUMBER WCO - 1060M

TO: RICKY L. WELTON, Special Agent, United States Army, Criminal Investigation Division,
and any Authorized Officer of the United States

Affidavit(s) having been made before me by RICKY L. WELTON, Special Agent, United States Army,
Criminal Investigation Division, and any Authorized Officer of the United States, who has reason to
believe that [] on the person of [X] on the premises known as

Information associated with kevinpelayo@hotmail.com, further described in Attachment A, that is stored
at premises controlled by Microsoft Corporation,

in the Western District of Texas there is now concealed a certain person or property, described on the
attached property list, see **Attachment B – List of Items to be Searched for and Seized**, which
property constitutes evidence of the commission of a criminal offense, contraband, the fruits of crime,
or things otherwise criminally possessed, property designed or intended for use or which is or has been
used as the means of committing a criminal offense concerning a violation of Title 18, United States
Code, Section 641.

I am satisfied that the affidavit(s) and any recorded testimony establish probable cause to believe that
the person or property so described is now concealed on the person or premises above-described and
establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before Within 14 days
(not to exceed 14 days) the person or place named above for the person or property specified, serving
the warrant and making the search (in the daytime - 6:00A.M. to 10:00 P.M.) (at any time in the day or
night as I find reasonable cause has been established) and if the person or property be found there to
seize same, leaving a copy of this warrant and receipt for the person or property taken and prepare a
written inventory of the person or property seized and promptly return this warrant to U.S. Magistrate
Judge as required by law.

June 8, 2020 @ 11:00 a.m.
Date and Time Issued

Waco, Texas
City and State

Jeffrey C. Manske, United States Magistrate Judge
Name and Title of Judicial Officer


Signature of Judicial Officer

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with kevinpelayo@hotmail.com that is stored at premises controlled by Microsoft Corporation, a company that accepts service of legal process at MSN Hotmail 1065 La Avenida, Building 4 Mountain View, CA 94043

ATTACHMENT B
Particular Things to Be Seized

I. Information to be disclosed by Microsoft Corp. (the Provider)

To the extent that the information associated with:

a) kevinpelayo@hotmail.com

Dating from October 1, 2018 to the present, as described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a requests made under 18 U.S.C. § 2703(f) on January 15, 2020 and April 16, 2020 the Provider is required to disclose the information described in paragraphs (a) through (f) below in this section to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the accounts, including stored or preserved copies of emails sent to and for the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and duration, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Providers and any person regarding the account, including contacts with support services and records of actions taken; and
- f. All records establishing control over or access to the subject email accounts.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. 641 (Theft), 18 U.S.C. 1028A (Aggravated Identify Theft), 18 U.S.C. 1343 (Wire Fraud), 18 U.S.C. 956(h) (Money Laundering), and 18 U.S.C. § 371 (Conspiracy), those violations involving known and unknown persons and occurring

after October 1, 2018, to the present including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. All data and records relating to names, emails and other identifying information for participants in relation to the Army Mass Transit Benefit Program (MTBP) to include but not limited to: creation of participant forms, payments for any U.S. government benefit, and claims in relation to the Army Mass Transit Benefit Program (MTBP).
- b. All data and records relating to claims submitted in relation to the Army Mass Transit Benefit Program.
- c. All data and records of payments relating to any U.S. Department of the Army, U.S. Department of Transportation, or U.S. Department of Defense claim, benefit, voucher, application, participant inquiries, and/or application forms in relation to the MTBP
- d. All data and records relating to agreements, drafts of agreements and proposed but unconsummated agreements related to the Army Mass Transit Benefit Program.
- e. All data and records identifying communications devices and numbers utilized during the formulation and submission of any U.S. government claim, or benefit, and application related to the Army MTBP, including residential telephones, fax machines, cell phones, blackberries, and like devices, address books, calendars, and other similar types of records.
- f. All data and records relating to financial accounts associated with Kevin Pelayo, Soldiers Van Pools, LLC, and the Army Mass Transit Benefit Program.
- g. All data, records and communications that may identify any co-conspirators of Kevin Pelayo or Soldiers Van Pools, LLC related to the Army Mass Transit Benefit Program.
- h. Email and attachments that provide context to any electronic mail reflecting the criminal activity described in this warrant including any electronic mail sent or received in temporal proximity to any relevant electronic mail and any electronic mail that identifies any users of the subject accounts; and
- i. Information relating to who created, used, or communicated with the accounts, including records about their identities and whereabouts.
- j. Any data and records pertaining to any communications with a government email address ending in .civ@mail.mil or .mil@mail.mil

III. Providers Procedures

Microsoft Corporation shall deliver the information set forth above within 30 days of the service of this warrant and shall send the information to:

U.S. Army CID-MPFU
Attn: Special Agent Ricky Welton
40 N.E. Loop 410
Suite #430
San Antonio, TX 78216
Ricky.L.Welton2.civ@mail.mil

FILED

SEALED

JUN - 8 2020

CLERK, U.S. DISTRICT COURT
WESTERN DISTRICT OF TEXAS
BY *cmw*
DEPUTY CLERK

United States District Court

WESTERN DISTRICT OF TEXAS

In the Matter of the Search of

Information associated with
kevinpelayo@hotmail.com, further described in
Attachment A, that is stored at premises controlled
by Microsoft Corporation

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: *W: 20-106m*

I, RICKY L. WELTON, being duly sworn depose and say: I am a(n) Special Agent, United States Army, Criminal Investigation Division, and have reason to believe that on the property or premises known as:

Information associated with kevinpelayo@hotmail.com, further described in Attachment A, that is stored at premises controlled by Microsoft Corporation,

in the Western District of Texas there is now concealed a certain person or property, described on the attached property list, **see Attachment B – List of Items To Be Searched for and Seized**, which property constitutes evidence of the commission of a criminal offense, contraband, the fruits of crime, or things otherwise criminally possessed, property designed or intended for use or which is or has been used as the means of committing a criminal offense concerning a violation of Title 18, United States Code, Section 671.

The facts to support a finding of Probable Cause are as follows:

Attached Affidavit of Special Agent Ricky L. Welton

Yes No



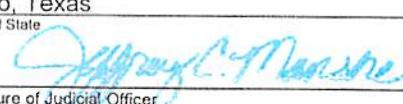
RICKY L. WELTON, Special Agent
United States Army
Criminal Investigation Division

Sworn to before me, and subscribed in my presence

June 8, 2020
Date

Jeffrey C. Manske, US Magistrate Judge
Name and Title of Judicial Officer

Waco, Texas
City and State


Signature of Judicial Officer

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with kevinpelayo@hotmail.com that is stored at premises controlled by Microsoft Corporation, a company that accepts service of legal process at MSN Hotmail 1065 La Avenida, Building 4 Mountain View, CA 94043

ATTACHMENT B

Particular Things to Be Seized

I. Information to be disclosed by Microsoft Corp. (the Provider)

To the extent that the information associated with:

- a) kevinpelayo@hotmail.com

Dating from October 1, 2018 to the present, as described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a requests made under 18 U.S.C. § 2703(f) on January 15, 2020 and April 16, 2020 the Provider is required to disclose the information described in paragraphs (a) through (f) below in this section to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the accounts, including stored or preserved copies of emails sent to and for the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and duration, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Providers and any person regarding the account, including contacts with support services and records of actions taken; and
- f. All records establishing control over or access to the subject email accounts.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. 641 (Theft), 18 U.S.C. 1028A (Aggravated Identity Theft), 18 U.S.C. 1343 (Wire Fraud), 18 U.S.C. 956(h) (Money Laundering), and 18 U.S.C. § 371 (Conspiracy), those violations involving known and unknown persons and occurring

after October 1, 2018, to the present including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. All data and records relating to names, emails and other identifying information for participants in relation to the Army Mass Transit Benefit Program (MTBP) to include but not limited to: creation of participant forms, payments for any U.S. government benefit, and claims in relation to the Army Mass Transit Benefit Program (MTBP).
- b. All data and records relating to claims submitted in relation to the Army Mass Transit Benefit Program.
- c. All data and records of payments relating to any U.S. Department of the Army, U.S. Department of Transportation, or U.S. Department of Defense claim, benefit, voucher, application, participant inquiries, and/or application forms in relation to the MTBP
- d. All data and records relating to agreements, drafts of agreements and proposed but unconsummated agreements related to the Army Mass Transit Benefit Program.
- e. All data and records identifying communications devices and numbers utilized during the formulation and submission of any U.S. government claim, or benefit, and application related to the Army MTBP, including residential telephones, fax machines, cell phones, blackberries, and like devices, address books, calendars, and other similar types of records.
- f. All data and records relating to financial accounts associated with Kevin Pelayo, Soldiers Van Pools, LLC, and the Army Mass Transit Benefit Program.
- g. All data, records and communications that may identify any co-conspirators of Kevin Pelayo or Soldiers Van Pools, LLC related to the Army Mass Transit Benefit Program.
- h. Email and attachments that provide context to any electronic mail reflecting the criminal activity described in this warrant including any electronic mail sent or received in temporal proximity to any relevant electronic mail and any electronic mail that identifies any users of the subject accounts; and
- i. Information relating to who created, used, or communicated with the accounts, including records about their identities and whereabouts.
- j. Any data and records pertaining to any communications with a government email address ending in .civ@mail.mil or .mil@mail.mil

III. Providers Procedures

Microsoft Corporation shall deliver the information set forth above within 30 days of the service of this warrant and shall send the information to:

U.S. Army CID-MPFU
Attn: Special Agent Ricky Welton
40 N.E. Loop 410
Suite #430
San Antonio, TX 78216
Ricky.L.Welton2.civ@mail.mil

SEALED

FILED

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

CLERK, U.S. DISTRICT COURT
WESTERN DISTRICT OF TEXAS
BY JMum
DEPUTY CLERK

I, Ricky L. Welton being first duly sworn hereby depose and state as follows:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Microsoft Corporation. (MSN), an email provider headquartered at 1065 La Avenida, Building 4 Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft Corporation to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.
2. I am a Special Agent with the U.S. Army Criminal Investigation Division's Major Procurement Fraud Unit (Army CID - MPFU) and have been employed with Army CID since April 2020. I am a federal law enforcement officer of the United States and I am authorized by law to conduct investigations and make arrests for felony offenses. Since on or about April 2019, I have been assigned to a unit specializing in investigations of fraud against the United States Army, bribery of public officials, conflict of interest, and money laundering. Prior to my employment as a Special Agent with Army CID - MPFU, I was a Deputy U.S. Marshal for approximately 14 years. During my tenure, I have worked complex cases, and thus I am familiar with the techniques, strategies, and behavior of individuals who have defrauded the government, and who seek to

conceal such illicit activities from detection by law enforcement. In many of the different types of crimes I have investigated, it has been common to seize and search electronic media, including personal computers, cellular phones, and gaming consoles all containing email, instant messaging and text messaging. I have used the information discovered on these electronic media to find communications among suspects, co-conspirators, and their victims, to find evidence of their criminal activity, and to identify suspects' other email/online identities as well as their co-conspirators and/or victims. I have used this information to aid in the successful prosecution of numerous suspects.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is Probable Cause to believe that Kevin Pelayo (hereafter **K. Pelayo**) and others Conspired to defraud the United States in violation of 18 U.S.C. § 371; Theft of money from the U.S. Government in violation of 18 U.S.C. § 641; Aggravated Identity Theft in violation of 18 U.S.C. § 1028A; Money Laundering in violation of 18 U.S.C. § 956(h), and devised a scheme to obtain money by false or fraudulent pretenses to be transmitted by means of wire in violation of 18 U.S.C. § 1343.

Purpose of Affidavit

5. This affidavit is made in support of a search warrant for email account

kevinpelayo@hotmail.com

Jurisdiction

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b) (l) (A) and (c) (l) (A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, 18 U.S.C. § 2711(3) (A) (i).

Probable Cause

7. Special Agents with U.S. Army CID are conducting an investigation into allegations that K. Pelayo stole approximately \$2.3 million dollars or more while serving as the Point of Contact (POC) for the Army Mass Transit Benefit Program (MTBP) at Fort Hood, TX. Kevin Pelayo fraudulently claimed numerous participants of the MTBP used the services of his company, Soldiers Van Pools, LLC, from October 2018 to August 2019. Evidence suggests that Kevin Pelayo used the names and personally identifiable information (PII) of soldiers, without their authorization, knowledge, or consent, to claim benefits that went directly to his company Soldiers Van Pools, LLC.

8. On or around October 2019 Mr. Quinn, Systems Analyst, U.S. Army Finance Command contacted K. Pelayo to conduct an audit for the Ft. Hood, Texas MTBP. During the conversation, K. Pelayo stated that he did not have any records and that he destroyed all of the records after he retired from active duty on August 1, 2019. Mr. Quinn was concerned with the amount of participants on Ft. Hood, Texas and the amount of money that was being disbursed to Soldiers Van Pools, LLC. Records indicated that approximately 1,079 participants were signed up for the Ft. Hood, Texas MTBP.

9. Mr. Quinn was concerned that no records were on file and that several participants were not stationed on Ft. Hood, Texas during the time that K. Pelayo submitted those names to the

Department of Transportation. K. Pelayo was an active duty soldier of the U.S. Army from approximately October 1997 to August 1, 2019. K. Pelayo retired under honorable conditions as a Sergeant First Class.

10. While stationed at Fort Hood, TX, K. Pelayo served as the Point of Contact (POC) for the Army Mass Transit Benefit Program where he was responsible for the overall operation of the program at Fort Hood, TX which included awareness of the program, accepting applications, sending applicant's information to the Department of Transportation, managing fare media, maintaining records of participants, reporting misuse and maintaining proper internal controls.

11. On October 1, 2019 the Ft. Hood, Texas CID Office was notified by Mr. Jerre Quinn, Financial Management Systems Analyst, Army Financial Services, Indianapolis, IN to report possible fraud conducted by K. Pelayo. Mr. Quinn stated his office attempted to coordinate with the Local Program Manager (LPM) at Fort Hood, TX. However, attempts to contact the LPM via email were unsuccessful. Mr. Quinn stated his office then contacted the owner of the local van pool, at which point they realized SFC (ret) Pelayo was both the LPM and the owner of the local van pool company, Soldiers Vanpools LLC. Mr. Quinn stated that SFC Pelayo said he no longer has the attendance schedules for the local MTBP participants.

12. Records from the Department of Defense (DOD) Manpower Data Center, who maintains personnel records for the DOD that K. Pelayo listed address, phone and email as 5007 Onion Rd. Killeen, Texas, phone number (253) 232-5392, and email kevinpelayo@hotmail.com

13. Your affiant obtained records from Hickam FCU and a review of those records revealed that on June 7, 2017, K. Pelayo sent an email to Member Services of Hickam FCU using kevinpelayo@hotmail.com to request an address change. K. Pelayo requested his address change from 4501 Lonesome Dove Drive, Killeen, Texas to 5007 Onion Road, Killeen, Texas.

14. Your affiant obtained records from the Texas Comptroller's Office and a review of those records revealed that on May 11, 2018, Cristine Fredericks, wife of K. Pelayo filed a Texas Franchise Tax Public Information Report with the Texas State Comptroller's Office, in Austin, Texas updating her business Title to Owner for Soldiers Van Pools, LLC. K. Pelayo was named as Director. The physical address for Soldiers Van Pools, LLC is 5007 Onion Rd, Killeen, Texas 76549 which is their primary residence. Cristine Fredericks resides with K. Pelayo at 5007 Onion Rd. Killeen, Texas 76549.

15. On August 1, 2019, K. Pelayo retired from the U.S. Army. According to Department of Transportation database records, on October 1, 2018 Soldiers Vanpools, LLC was registered to do business with the U.S. Army Mass Transit Benefit Program on Ft. Hood, Texas. The Business Point of Contact was listed as K. Pelayo. Prior to retirement K. Pelayo used his official government email address to send and receive correspondence. On August 20, 2019 K. Pelayo used the email address: kevionpelayo@hotmail.com as a business point of contact email.

16. Your affiant obtained records from the Defense Information Systems Agency indicating that on August 20, 2019, K. Pelayo sent an email to an individual named J. Peavy using kevinpelayo@hotmail.com J. Peavy is an active duty soldier that was named as an alternate point of contact for the Ft. Hood, Texas MTBP. The email from K. Pelayo contained an excel spread sheet of the names of alleged participants for the month of August 2019 for the Ft. Hood, Texas MTBP. K. Pelayo did not have access to his official Army e-mail account due to his retirement on August 1, 2019 and had J. Peavy use his official Army e-mail to send the information to the Department of Transportation. It is unknown how K. Pelayo was able to get the names of the soldiers and their information after his retirement on August 1, 2019.

17. Your affiant obtained records from the Department of Public Safety which reflected on February 4, 2020 K. Pelayo updated his Texas Driver's License and provided kevinpelayo@hotmail.com. Furthermore, bank records show that K. Pelayo was still receiving payments for the MTBP after his retirement from the Army on August 1, 2019. K. Pelayo would not have access to any official Army e-mail after retirement and would have to use kevinpelayo@hotmail.com for any business associated with Soldiers Van Pools, LLC. Additionally, on March 12, 2020 Texas DPS verified that Bell County, Texas records show K. Pelayo has been residing at 5007 Onion Road Killeen, Texas since approximately June 9, 2017.

18. According to U.S. Army MTBP (Outside the National Capital Region) policy, procedures and guidelines, the term Point of Contact (POC) refers to a person designated by the Army to ensure proper execution of the MTBP in accordance with Executive Order 13150 and Headquarters Department of Army policy guidance as well as among other things.

19. The Army policy further directed that K. Pelayo, as a MTBP POC, was to establish and maintain a list of available van pool vendors in and around Ft. Hood, Texas. No information has been received indicating that K. Pelayo did this considering majority of the names provided allegedly used Soldiers Van Pools, LLC. SA Welton was able to interview several soldiers to verify the validity of the participants using Soldiers Van Pools, LLC as their vanpool provider. Most soldier's interviewed stated that they did not sign up for this program and that they were not aware that they were even enrolled in the program. As the point of contact for Ft. Hood, Texas, K. Pelayo was supposed to accept applications from both civilian and military soldiers for enrollment in the MTBP. K. Pelayo was then to review the applications for accuracy, verify and approve applicants' eligibility into participate in the program, review commuter expenses, and submit the applicant's information to DOT, using the MTPB Application Submission Form (Excel spread sheet), arrange

for distribution of fare media when applicable, and provide information to participants of any changes to fare media. Additionally, K. Pelayo was to maintain records of expenditures and provide them to the Department of Army Program Point of Contact annually for audit purposes. K. Pelayo was unable to provide any information to Army Finance as indicated by Mr. Quinn. The main reason for Army Finance Command contacting K. Pelayo was to audit the participants that were submitted by K. Pelayo. Finally, no information was provided to Army Finance Command from K. Pelayo in reference to his company Soldiers Van Pools, LLC.

Investigation of Alleged Criminal Activity

20. The Army CID Office on Ft. Hood, Texas informed our office that the Army Finance Command reported irregularities with the Fort Hood MTBP. According to Special Agent Perkins of the Fort Hood CID Office, on or about October 1, 2019, Mr. Jerre Quinn, a Systems Analyst from Army Finance Command attempted to collect the required MTBP paperwork from K. Pelayo and was unsuccessful. K. Pelayo stated to Mr. Quinn that he (Kevin Pelayo) destroyed all paperwork relating to the Ft. Hood MTBP after he retired. Mr. Quinn stated that he was suspicious of the volume of participants being registered at Ft. Hood, Texas as compared to other military installations outside of the Capital Region. Mr. Quinn became suspicious that numerous participants maybe using a company owned and operated by K. Pelayo and C. Fredericks. Army Finance Command also questioned whether or not K. Pelayo was able to provide the amount of transportation required to transport the participants.

21. On December 10, 2019 Mr. Quinn was interviewed by SA Welton and advised requesting the paperwork to conduct an audit as required by Army Finance Command policy. Mr. Quinn also stated that numerous participants that are on the Ft. Hood MTBP are not even stationed on Ft. Hood and that K. Pelayo showed to be stationed in Korea at the time of majority of these

transactions. Mr. Quinn also realized that majority of the participants payments were going directly to Soldiers Vanpools LLC, which is owned and operated by K. Pelayo and C. Fredericks. Mr. Quinn also stated that after his conversation with K. Pelayo in August 2019, his office cancelled all of the participants under K. Pelayo and his company Soldiers Van Pools, LLC. This did not stop K. Pelayo from conducting his fraudulent activities. Bank records indicated that after Mr. Quinn cancelled all of the participants that K. Pelayo was still receiving monthly payments for the program. A request was sent to Army Finance Command to identify the participants which is ongoing. K. Pelayo had to use his personal email account to send and receive information for Soldiers Van Pools, LLC.

22. Mr. Quinn stated that using your own company and being the POC is against policy because the point of contact for the MTBP cannot have any influence towards a certain company or own a company that directly profits from this program. Furthermore, every point of contact has to be stationed on the base they are assigned to in order to be a point of contact for that particular base. K. Pelayo was stationed in South Korea in 2018 until his retirement on August 1, 2019.

23. Mr. Quinn said that K. Pelayo was to send in a withdraw form to the Department of Transportation relinquishing himself as the program point of contact once he transferred to Korea. K. Pelayo failed to notify the Department of Transportation and the U.S. Army Finance Command of his transfer to South Korea. K. Pelayo was still sending in participant names while he was stationed in South Korea to benefit his business. Also, many of the participants were not aware that they were signed up for this program and that their name and personal identification information was used to sign them up and receive claims without their knowledge, consent, or authorization.

September 2019	XXXX2010	\$276,725.00
October 2019	XXXX2010	\$47,605.00

26. On August 20, 2019, K. Pelayo sent an email from his private Hotmail email address (kevinpelayo@hotmail.com) to J. Peavy at email address (joseph.w.peavy.mil@mail.mil) with the subject Ft. Hood MTBP Aug 19. The body of the email starts with Brother, here is the list that need to be sent to Jessica at Jessica.dunlap@dot.gov. Attached to the email was an excel spreadsheet with several names of U.S. Army soldiers, the last four of their social security number, command, fare media requested, which was debit card, monthly amount requested, work phone, common identifier, work zip code, eligibility date, and transit mode.

Total Enrolling: 11

LAST NAME	FIRST NAME	MI	LAST 4 SSN	COMMAND	EMPLOYEE TYPE								NAF ONLY	FARE MEDIA	MONTHLY AMOUNT REQUESTED		
					ARMY		ARMY NATIONAL GUARD		ARMY RESERVE		NAF						
					CIV	OFF	ENL	CIV	OFF	ENL	CIV	OFF	ENL	SNN			
Sharpe	Scott	A	9266	FORSCOM			x									debit card	\$ 265.00
Capeillo	Joseph	F	9375	FORSCOM		x										debit card	\$ 265.00
Shanahan	Jordan	K	2465	FORSCOM			x									debit card	\$ 265.00
Garza	Steven	A	3358	FORSCOM			x									debit card	\$ 265.00
Arsola	Joseph	M	3827	FORSCOM			x									debit card	\$ 265.00
Dietrich	Colt	A	7252	FORSCOM			x									debit card	\$ 265.00
Burns	Anthony	W	5705	FORSCOM			x									debit card	\$ 265.00
Townsend	Gabriel	V	6923	FORSCOM			x									debit card	\$ 265.00
Charles	Clarence	B	9211	FORSCOM			x									debit card	\$ 265.00
Velasco	Vaugez	D	1976	FORSCOM			x									debit card	\$ 265.00
Robinson	Thomas	T	7481	FORSCOM			x									debit card	\$ 265.00

27. On February 12, 2020 your affiant obtained and reviewed the Defense Enterprise email account of a SFC Joseph Peavy. SFC Peavy used his official government email account to send an email to the Department of Transportation in reference to the August 2019 Ft. Hood MTBP

received by K. Pelayo's Hotmail account. A review of the U.S. Army email account disclosed communications from SFC Peavy and K. Pelayo indicating that the list attached in the email needed to be sent to Jessica Dunlap, an employee with the Department of Transportation, who coordinates the Mass Transit Benefit Program for the U.S. Army.

28. On 20 Feb 2020 your affiant interviewed SFC Arsola who stated that he is currently stationed at Ft. Sill, OK. SFC Arsola stated that he has never been stationed on Ft. Hood, Texas. SFC Arsola stated he never completed any information for any van pool or rideshare program. SFC Arsola did not recall the name Kevin Pelayo or the company Soldiers Van Pools, LLC. SFC Arsola was previously identified as an alleged participant in the Mass Transit Benefit Program (MTBP) on Ft. Hood, Texas for the month of September 2019 where \$265 was allocated to be paid to Soldiers VanPools, LLC. No payment was transferred due to Army Finance Command cancelling all participants associated with Kevin Pelayo and Soldiers Van Pools, LLC.

29. On 29 Feb 2020 your affiant interviewed SFC Sharpe stated that he is currently training in Germany. SFC Sharpe stated that he is stationed on Ft. Hood, Texas with 1st Cav Division. SFC Sharpe stated he never completed any information for any van pool or rideshare program. SFC Sharpe did not recall the name Kevin Pelayo or the company Soldiers Van Pools, LLC. SFC Sharpe was previously identified as an alleged participant in the Mass Transit Benefit Program (MTBP) on Ft. Hood, Texas for the month of September 2019 where \$265 was allocated to be paid to Soldiers VanPools, LLC. No payment was transferred due to Army Finance Command cancelling all participants associated with Kevin Pelayo and Soldiers Van Pools, LLC.

30. On March 30, 2020 your affiant requested subscriber information for kevinpelayo@hotmail.com to verify if this email address.

31. On May 11, 2020 your affiant received and reviewed subscriber information from Microsoft Corporation which reflected kevinpelayo@hotmail.com was created on September 12, 1999 in New York from postal code 10956. This zip code comes back to New City, NY. Kevin Pelayo's mother lives at 8 Ruth Dr. New City, NY and this is where K. Pelayo entered the Army from as indicated on his military record. An alternate email of kevin.pelayo@us.army.mil was provided. A request of his military email account was unsuccessful due to records only being on file for 120 days after retirement.

32. Your affiant knows that it is against government policy for a U.S. Army soldier such as K. Pelayo to send information like this over an unsecured personal email. This information was sent over his private email account because K. Pelayo was already retired from the U.S. Army and did not have access to his government email account. K. Pelayo was not eligible to send in any participant applications because the point of contact has to be an active duty soldier or civilian worker that either works on Ft. Hood or is an active duty soldier stationed on Ft. Hood.

Preservation Letter

33. On January 15, 2020, and April 16, 2020 a preservation letter was sent to Microsoft for the account kevinpelayo@hotmail.com. In general, an email that is sent to a Microsoft subscriber is stored in the subscriber's "mail box" on Microsoft servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Microsoft servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Microsoft's servers for a certain period of time.

Background Concerning Email

34. In my training and experience, I have learned that Microsoft provides a variety of on-line services, including electronic mail (email) access, to the public. Subscribers obtain an account by

registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain stored electronic communications (including retrieved and un-retrieved) email for Microsoft subscribers and information concerning subscribers and their use of Microsoft services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

35. A Microsoft subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by Microsoft Corporation. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, emails in the account, and attachments to emails, including pictures and files.

36. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

37. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log in (i.e., session) times and durations, the types of service until the status of the account (including whether

the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

38. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the providers support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the accounts user or users.

Conclusion

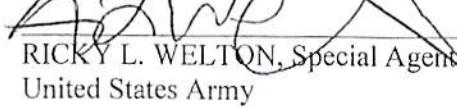
39. Based upon the foregoing facts and upon Affiant's training and experience, there is evidence to believe that K. Pelayo conspired with others to defraud the U.S. Army when he obtained the names and personal information of soldiers and submitted them to the Department of Transportation without their knowledge, consent, or authority by using his personal email account kevinpelayo@hotmail.com. Furthermore, K. Pelayo used the names for his benefit by indicating to the Department of Transportation that all of the participants that he submitted were going to use his personal business Soldiers Vanpools LLC. K. Pelayo abused the Army MTBP system and used

numerous names without the consent, knowledge, or authority of the named participants for personal financial gain.

40. Evidence further supports K. Pelayo conspired with others to defraud the U.S. Army when he obtained the names and personal information from soldiers to use for his financial gain by using his personal email account. K. Pelayo did willfully and knowingly participate personally and substantially as a U.S. Army MTBP point of contact for Ft. Hood, Texas even after he retired from the Army knowing that this was against Army policy. Based upon the foregoing facts and the affiants training and experience, the nature of government programs, the size of government programs and related personnel, communications, payments and other activity K. Pelayo would have used his personal Microsoft email account to facilitate and engage in the criminal activity described above.

Request for Sealing

41. I further request that the Court order that all papers in support of this application including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.


RICKY L. WELTON, Special Agent
United States Army
Criminal Investigation Division

SWORN TO AND SUBSCRIBED before me on the 8th day of June, 2020.


JEFFREY C. MANSKE
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with kevinpelayo@hotmail.com that is stored at premises controlled by Microsoft Corporation, a company that accepts service of legal process at MSN Hotmail 1065 La Avenida, Building 4 Mountain View, CA 94043

ATTACHMENT B
Particular Things to Be Seized

I. Information to be disclosed by Microsoft Corp. (the Provider)

To the extent that the information associated with:

- a) kevinpelayo@hotmail.com

Dating from October 1, 2018 to the present, as described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a requests made under 18 U.S.C. § 2703(f) on January 15, 2020 and April 16, 2020 the Provider is required to disclose the information described in paragraphs (a) through (f) below in this section to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the accounts, including stored or preserved copies of emails sent to and for the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and duration, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Providers and any person regarding the account, including contacts with support services and records of actions taken; and
- f. All records establishing control over or access to the subject email accounts.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. 641 (Theft), 18 U.S.C. 1028A (Aggravated Identify Theft), 18 U.S.C. 1343 (Wire Fraud), 18 U.S.C. 956(h) (Money Laundering), and 18 U.S.C. § 371 (Conspiracy), those violations involving known and unknown persons and occurring

after October 1, 2018, to the present including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. All data and records relating to names, emails and other identifying information for participants in relation to the Army Mass Transit Benefit Program (MTBP) to include but not limited to: creation of participant forms, payments for any U.S. government benefit, and claims in relation to the Army Mass Transit Benefit Program (MTBP).
- b. All data and records relating to claims submitted in relation to the Army Mass Transit Benefit Program.
- c. All data and records of payments relating to any U.S. Department of the Army, U.S. Department of Transportation, or U.S. Department of Defense claim, benefit, voucher, application, participant inquiries, and/or application forms in relation to the MTBP
- d. All data and records relating to agreements, drafts of agreements and proposed but unconsummated agreements related to the Army Mass Transit Benefit Program.
- e. All data and records identifying communications devices and numbers utilized during the formulation and submission of any U.S. government claim, or benefit, and application related to the Army MTBP, including residential telephones, fax machines, cell phones, blackberries, and like devices, address books, calendars, and other similar types of records.
- f. All data and records relating to financial accounts associated with Kevin Pelayo, Soldiers Van Pools, LLC, and the Army Mass Transit Benefit Program.
- g. All data, records and communications that may identify any co-conspirators of Kevin Pelayo or Soldiers Van Pools, LLC related to the Army Mass Transit Benefit Program.
- h. Email and attachments that provide context to any electronic mail reflecting the criminal activity described in this warrant including any electronic mail sent or received in temporal proximity to any relevant electronic mail and any electronic mail that identifies any users of the subject accounts; and
- i. Information relating to who created, used, or communicated with the accounts, including records about their identities and whereabouts.
- j. Any data and records pertaining to any communications with a government email address ending in .civ@mail.mil or .mil@mail.mil

III. Providers Procedures

Microsoft Corporation shall deliver the information set forth above within 30 days of the service of this warrant and shall send the information to:

U.S. Army CID-MPFU
Attn: Special Agent Ricky Welton
40 N.E. Loop 410
Suite #430
San Antonio, TX 78216
Ricky.L.Welton2.civ@mail.mil